

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.

H04W 12/08 (2009.01)



[12] 发明专利说明书

专利号 ZL 03818493.1

[45] 授权公告日 2009 年 12 月 30 日

[11] 授权公告号 CN 100576956C

[22] 申请日 2003.8.11 [21] 申请号 03818493.1

[30] 优先权

[32] 2002.8.13 [33] US [31] 60/403,158

[86] 国际申请 PCT/US2003/025131 2003.8.11

[87] 国际公布 WO2004/015968 英 2004.2.19

[85] 进入国家阶段日期 2005.2.1

[73] 专利权人 汤姆森许可贸易公司

地址 法国布洛里

[72] 发明人 谢利·维尔马 查尔斯·传铭·王
张军标

[56] 参考文献

US5920814A 1999.7.6

CN1227688A 1999.9.1

US6167279A 2000.12.26

审查员 吴翔晖

[74] 专利代理机构 中科专利商标代理有限责任公
司

代理人 戎志敏

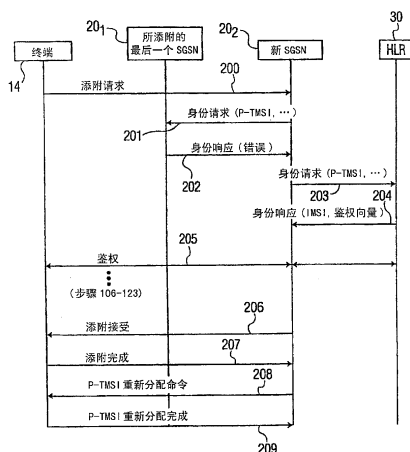
权利要求书 2 页 说明书 8 页 附图 3 页

[54] 发明名称

通过归属位置寄存器修改的移动终端身份保
护

[57] 摘要

通过使归属位置寄存器(30)存储终端的临时和永久身份来实现通过无线网络(10)的移动无线终端(14)的安全接入。当在初始注册之后接入网络时,终端向服务 GPRS 支持节点(SGSN)(201 和 202)发送临时身份。如果没有网络中的服务节点知道终端,终端不需要如之前所需地以明文发送其永久身份。而是由于 HLR 能够将终端的临时身份映射到其永久身份,服务节点只需查询 HLR。按照这种方式,移动无线终端的永久身份保持了安全。



1. 一种用于在添附到无线网络期间保护移动无线终端的身份的方法，包括步骤：

在网络中接收到来自之前注册到网络的移动无线终端的接入请求；

根据包含在接入请求中的临时身份来查询无线网络中至少一个服务节点，以辨认移动无线终端，如果没有服务节点辨认出移动无线终端，则

从至少一个服务节点发起向无线网络中存储了之前注册的移动无线终端的身份信息的寄存器的查询，以根据其临时身份识别移动无线终端；以及

从寄存器向发起查询的服务节点发送包括移动无线终端的永久身份信息 IMSI 和验证终端所需的相关鉴权矢量的标识响应，以识别移动无线终端。

2. 根据权利要求 1 所述的方法，其特征在于还包括步骤：当每一次分配了移动无线终端的临时身份时，更新寄存器，其中，分配包括第一次分配和重新分配。

3. 根据权利要求 1 所述的方法，其特征在于还包括步骤：在移动无线终端离开无线网络时，更新寄存器。

4. 根据权利要求 1 所述的方法，其特征在于当从终端接收到离开请求和应答时，至少一个服务节点丢弃所存储的用于所述终端的临时身份。

5. 根据权利要求 4 所述的方法，其特征在于还包括步骤：当移动无线终端发起离开时，在至少一个服务节点中存储包含在离开请求中的临时身份。

6. 根据权利要求 3 所述的方法，其特征在于还包括步骤：当无线

电话网络发起与移动无线终端的分离时，在临时身份重新分配之后，存储移动无线终端的新的临时身份。

7. 根据权利要求 1 所述的方法，其特征在于还包括步骤：在临时身份重新分配之后，在寄存器中存储移动无线终端的新和旧临时身份。

8. 一种用于在添附期间保护移动无线终端的身份的无线网络，包括：

至少一个服务节点，用于接收来自之前注册到网络的移动无线终端的接入请求，并且当服务节点具有所述终端的知识时，根据包含在接入请求中的临时身份来识别终端；以及

无线网络中的寄存器，当一个服务节点缺乏终端的知识时，响应来自一个服务节点的查询，存储之前注册的移动无线终端的永久身份信息，使用移动无线终端的永久身份信息从其临时身份来识别所述移动无线终端；

寄存器向发起查询的服务节点发送移动无线终端的永久身份信息 IMSI 和验证终端所需的相关鉴权矢量的标识响应。

9. 根据权利要求 8 所述的网络，其特征在于当每一次分配了移动无线终端的临时身份时，更新寄存器。

10 根据权利要求 8 所述的网络，其特征在于在移动无线终端离开无线网络时，对寄存器进行更新。

11. 根据权利要求 10 所述的网络，其特征在于当从终端接收到离开请求和应答时，至少一个服务节点丢弃所存储的用于所述终端的临时身份。

12. 根据权利要求 11 所述的网络，其特征在于当移动无线终端发起离开时，至少一个服务节点存储包含在离开请求中的临时身份。

13. 根据权利要求 12 所述的网络，其特征在于当无线网络发起与移动无线终端的分离时，在临时身份重新分配之后，至少一个服务节点存储移动无线终端的新的临时身份。

14. 根据权利要求 8 所述的网络，其特征在于在临时身份重新分配之后，寄存器存储移动无线终端的新和旧临时身份。

通过归属位置寄存器修改的移动终端身份保护

技术领域

本发明涉及一种当接入无线网络时用于保护移动无线终端的身份的技术。

背景技术

近年来，寻求无线电话服务的用户通常订阅这种服务的多个提供者之一。现在的无线电话服务提供者不仅提供语音呼叫，还提供通用分组无线服务（GPRS），以便能够通过移动无线终端交换数据分组。当 GPRS 存在于多个区域中时，数据传输率典型地不会超过 56Kbs 并且无线网络服务提供者支持该服务的成本保持在较高，这使得 GPRS 较昂贵。为了提供增强的数据通信，现在的努力在于建立用于无线电话的新标准。一种这样的努力是由第三代伙伴计划（3GPP）制订的建议“通用移动通信系统（UMTS）”标准，用于无线电话网络中的高级分组无线电服务。UMTS 标准建议了高达 2Mbps 的传输率，使得这种服务更吸引订户。

根据 UMTS 标准，当初始注册时，订户的移动无线终端向网络发送典型地被称作国际移动台身份或 IMSI 的永久身份。为了保持用户身份的机密性和不可跟踪性，在初始注册之后，每一个订户从无线网络接收在网的服务 GPRS 支持节点（SGSN）保存的、被称作分组临时移动订户身份（P-TMSI）的临时身份。当随后每一次接入无线网络时，移动无线终端发送其 P-TMSI。服务于移动无线终端的 SGSN 将 P-TMSI 映射到用户的永久身份（即，IMSI）。按照这种方式，用户避免了发送其 IMSI。为了减小破坏用户的机密性的危险，网络不应当利用相同的 P-TMSI 在较长的周期内识别用户。而是应当由无线电话网络在某一延长的时间间隔之后分配新的 P-TMSI。

尽管努力通过 P-TMSI 来保护用户的机密性，情况是现代的无线电话网络需要移动无线终端在注册之后发送其永久身份（IMSI）。例如，当向无线电话网络进行新的添附时，移动无线终端会遭遇到与在分开之前服务于该终端的 SGSN 不同的 SGSN。当是这样的新添附时，移动无线终端向新的 SGSN 发送其 P-TMSI。随后，新的 SGSN 向旧 SGSN 发送标识请求消息。如果旧和新 SGSN 均缺乏移动无线终端的知识，新 SGSN 向终端发送身份请求。移动无线终端必须利用其明文永久身份（IMSI）进行响应，破坏了用户身份的机密性。

因此，需要用于在添附到无线电话网络期间保护用户身份的技术。

发明内容

本发明的目的是提供一种能够使移动无线终端安全地接入例如无线电话网络的无线网络的方法。

按照本发明的一方面，一种用于在添附到无线网络期间保护移动无线终端的身份的方法，包括步骤：

在网络中接收到来自之前注册到网络的移动无线终端的接入请求；

根据包含在接入请求中的临时身份来查询无线网络中至少一个服务节点，以辨认移动无线终端，如果没有服务节点辨认出移动无线终端，则

从至少一个服务节点发起向无线网络中存储了之前注册的移动无线终端的身份信息的寄存器的查询，以根据其临时身份识别移动无线终端；以及

从寄存器向发起查询的服务节点发送包括移动无线终端的永久身份信息 IMSI 和验证终端所需的相关鉴权矢量的标识响应，以识别移动无线终端。

按照本发明的另一方面，一种用于在添附期间保护移动无线终端的身份的无线网络，包括：

至少一个服务节点，用于接收来自之前注册到网络的移动无线终端的接入请求，并且当服务节点具有所述终端的知识时，根据包含在

接入请求中的临时身份来识别终端；以及

无线网络中的寄存器，当一个服务节点缺乏终端的知识时，响应来自一个服务节点的查询，存储之前注册的移动无线终端的永久身份信息，使用移动无线终端的永久身份信息从其临时身份来识别所述移动无线终端；

寄存器向发起查询的服务节点发送移动无线终端的永久身份信息 IMSI 和验证终端所需的相关鉴权矢量的标识响应。

在归属位置寄存器中保存移动无线终端临时身份信息能够使不能辨认终端的服务节点查询寄存器。按照这种方式，当不能被服务节点辨认时，移动无线终端不需要发送其永久身份。

附图说明

图 1 示出了用于实现本发明发明的无线电话网络的演示实施例的方框示意图；

图 2 示出了移动无线终端将其自身添附到图 1 的网络的现有技术过程的步骤的图；以及

图 3 示出了根据本发明移动无线终端将其自身添附到图 1 的网络的过程的步骤的图。

具体实施方式

图 1 示出了具有与 UMTS 3GPP 标准所建议的相同结构的无线电话网络 10 的方框示意图。无线电话网络 10 包括至少一个，优选是多个无线电接入网络，如无线电接入网络 12₁ 和 12₂ 示意所示。在包括节点 B 和无线电网络控制器(RNC)的 UMTS 无线电接入网络中，UMTS 节点 B 用于寻求与（将其自身添附到）网络 10 连接的移动无线终端 14 的接入点。每一个无线电网络控制器（RNC）16₁ 和 16₂ 分别控制无线电接入网络 12₁ 和 12₂ 中独立的一个，用于在每一个网络中分配必要资源的目的。

每一个 RNC 16₁ 和 16₂ 分别与对应的一个服务 GPRS 支持节点（SGSN）20₁ 和 20₂ 相连，所述 SGSN 包括无线电话网络 10 的部分核

心。对于对应无线电接入网络的订户，每一个 SGSN 管理分组和语音服务。每一个 SGSN 具有到网关 GPRS 节点 (GGSN) 22 的链路，对于分组服务，所述 GGSN 作为到因特网 24 的接口。按照类似的方式，SGSN 20₁ 与移动交换中心 (MSC) 26 相连，对于语音服务，所述 MSC 连接了公共交换电话网 (PSTN) 28。类似的 MSC (未示出) 将 SGSN 20₂ 与 PSTN 28 相连。

在无线网络 10 中，存在典型被称作归属位置寄存器或 HLR 的至少一个寄存器 (数据库) 30。HLR 30 包含识别哪一个 SGSN 服务于具体订户的分组域订阅数据和位置信息。每一个 SGSN 20₁ 和 20₂ 通过独立的 Gr 接口访问 HLR 30，而 GGSN 22 通过 Gc 接口访问 HLR。根据本发明，HLR 30 存储之前添附到无线网络 10 的每一个移动无线终端 14 的国际移动台身份 (IMSI) 和临时身份 (P-TMSI)。此外，HLR 30 存储每一个 SGSN 的身份 (即，地址)、当前添附到移动无线终端 14 的 SGSN 的地址以及如果终端当前离开时所访问的最后一个 SGSN 的地址。对于不常驻无线网络 10 中的漫游移动无线终端 14，通过因特网 24 或专用线路 (未示出)，能够访问与位于不同无线电话网络的终端相关联的 HLR。

为了更好地理解通过本发明的添附技术获得的优点，首先给出图 2 所示当前添附技术的说明。当从一个无线电接入网络的覆盖区域移动到另一个时，移动无线终端 14 在图 2 的步骤 100 期间进行服务于新接入无线电接入网络的新 SGSN 的添附请求。出于演示的目的，假设移动无线终端 14 通过图 1 的无线电接入网 12₂ 来寻求添附。因此，移动无线终端 14 通过进行到以下被称为“新”SGSN 的 SGSN 20₂ 的添附请求来发起添附处理。如果新 SGSN 20₂ 没有移动无线终端 14 的身份信息，新 SGSN 在图 2 的步骤 102 期间将添附请求转发到“旧”SGSN (例如图 1 的 SGSN 20₁)。如果旧 SGSN 20₁ 不再保留用于移动无线终端 14 的任意身份信息，新 SGSN 在图 2 的步骤 103 期间接收身份响应，所述响应指示了旧 SGSN 缺乏移动无线终端 14 的知识。

当接收到来自旧 SGSN 20₁ 的指示，移动无线终端 14 仍然未知时，在图 2 的步骤 104 期间，新 SGSN 20₂ 向移动终端发送身份请求。如

果 SGSN 20₁ 和 SGSN 20₂ 都未知，则移动无线终端 14 不能简单地发送其 P-TMSI 以识别自身。相反，移动无线终端 14 必须在图 2 的步骤 105 期间通过以明文向新 SGSN 20₂ 发送其永久身份（即其 IMSI）来响应身份请求。以明文发送 IMSI 导致订户身份的被截获和欺诈滥用的危险。

当接收到 IMSI 之后，新 SGSN 20₂ 通过在图 2 的步骤 106 期间查询 HLR 30 来鉴权移动无线终端 14。当接收到来自 HLR 30 的肯定验证响应时，新 SGSN 20₂ 在步骤 107 期间向移动无线终端 14 提供肯定的验证响应。之后，移动无线终端 14 在图 2 的步骤 108 期间向新 SGSN 20₂ 发送国际移动设备身份（IMEI）请求，以发起终端位置的更新以及验证终端的状态。在接收到 IMEI 检查请求之后，新 SGSN 20₂ 在步骤 109 期间查询图 2 的设备身份寄存器 32，验证与被偷窃的相比移动无线终端 14 是否合法。当在步骤 109 期间发现移动无线终端 14 合法时，新 SGSN 20₂ 在步骤 110 期间向 HLR 30 发送消息，以更新终端的位置。

响应终端位置更新信息，HLR 30 在步骤 111 期间向旧 SGSN 20₁ 发送请求，以取消存储在其中的移动无线终端 14 的位置信息。在步骤 112 期间，旧 SGSN 20₁ 利用取消位置应答进行响应。在步骤 113 期间，HLR 30 将与现在将其自身添附到该 SGSN 的移动无线终端 14 相关联的订户数据插入到新 SGSN 20₂。在步骤 114 期间，新 SGSN 20₂ 利用插入订户数据应答进行响应。在步骤 114 之后，HLR 在图 2 的步骤 115 期间利用更新位置应答消息对新 SGSN 20₂ 进行响应。

由于由与旧 SGSN 20₁ 不同的 MSC 服务于新 SGSN 20₂，除了更新 HLR 30 以外，新 SGSN 20₂ 还在步骤 116 期间进行对图 1 的 MSC 26 的访问位置寄存器（VLR）（未示出）的更新请求。当接收到这种请求时，新 MSC/VLR 26 在步骤 117 期间进行请求以更新 HLR 30。随后，HLR 30 在步骤 118 期间向旧 MSC/VLR（表示为图 2 的 MSC 26'）发送取消命令，以指示移动无线终端到新 SGSN 20₂ 的添附。图 2 的旧 MSC 26' 在步骤 119 期间利用应答消息进行响应。

接下来，在步骤 120 期间，HLR 30 将已更新的订户数据插入新

MSC/VLR 26。新 MSC 26 在步骤 122 期间利用插入订户数据应答消息进行响应。然后，图 2 的新 MSC/VLR 26 在步骤 123 期间向新 SGSN 20₂ 发送位置更新接受消息，触发在步骤 124 期间从新 SGSN 到移动无线终端 14 的添附接受消息的发送。移动无线终端 14 在步骤 125 期间利用“添附完成”消息进行响应，之后是在步骤 126 期间从 SGSN 20₂ 到新 MSC/VLR 26 的 TMSI 重新分配完成消息，以指示从旧到新 SGSN 的 TMSI 映射的重新分配任务的完成。

图 2 的现有技术添附处理存在当旧 SGSN 20₁ 和新 SGSN 20₂ 都不能辨认终端时需要移动无线终端 14 以明文发送其 IMSI 的缺点。优选如图 3 所示，本发明的添附技术通过在 HLR 30 中存储订户身份信息克服了该缺点。在 HLR 30 中存储这种信息能够在新或旧 SGSN 都不能辨认终端的情况下进行移动无线终端 14 的标识。参考图 3，在终端转移到图 1 的无线接入网络 12₂ 之后，当移动无线终端 14 在步骤 200 期间向新 SGSN 20₂ 发送“添附请求”消息时，开始本发明的添附技术。当在图 3 的步骤 200 期间接收到“添附请求”消息时，新 SGSN 20₂ 在步骤 202 期间向旧 SGSN 20₁ 发送身份请求消息，以识别移动无线终端 14。如果缺乏已经添附的移动无线终端 14 的知识，旧 SGSN 20₁ 会在步骤 202 期间向新 SGSN 20₁ 发送指示了错误的身份响应消息。

以前，当旧 SGSN 20₁ 缺乏移动无线终端 14 的之前添附的知识时，终端需要以明文发送其永久身份以识别其自身。为了避免该缺点，本添附方法在这种环境下不进行移动无线终端 14 的请求。而是如图 3 所示。当在步骤 202 期间接收到错误消息之后，新 SGSN 20₂ 在步骤 203 期间向 HLR 寄存器 30 发送身份请求消息。根据本发明的发明，HLR 30 存储之前添附到无线网络 10 的每一个移动无线终端 14 的临时身份（即，P-TMSI）和永久身份（IMSI）。因此，当在步骤 203 期间接收到身份请求消息时，HLR 30 在步骤 204 期间向新 SGSN 20₂ 提供身份响应消息。该消息包括移动无线终端 14 的 IMSI 和验证终端所需的相关鉴权矢量。在步骤 205 期间，发生了移动无线终端 14 的鉴权。典型地，这种鉴权按照与图 2 的步骤 106-123 期间相同的方式进行。

鉴权之后,在图3的步骤206期间,新SGSN 20₂向移动无线终端14发送添附接受消息。作为响应,移动无线终端14在步骤207期间发送“添附完成”应答消息。在步骤208期间,新SGSN 20₂能够通过向移动无线终端14发送P-TMSI重新分配命令来重新分配P-TMSI。当P-TMSI的重新分配完成时,移动无线终端14在步骤209期间向新SGSN 20₂发送P-TMSI重新分配完成应答。

可用的GPRS和UMTS标准假设SGSN可以在任意时间重新分配P-TMSI。这种重新分配可以发生在P-TMSI重新分配过程中,或作为“添附”或“路由区域更新”过程的一部分。每一次更新HLR 30时,SGSN之一重新分配P-TMSI会消耗重要的资源。相反,只有在离开时,当接收到来自SGSN的P-TMSI和P-TMSI签名,才应当进行HLR更新,即,只有在将最后的P-TMSI和P-TMSI签名存储在HLR 30中时。当SGSN向移动无线终端14发出新P-TMSI以替换旧P-TMSI时,在去除旧P-TMSI并使用新P-TMSI之前,SGSN等待应答。

在实际中,当接收到P-TMSI重新分配完成应答消息时,图1的无线电话网络认为旧P-TMSI无效。出于某种原因,如果SGSN没有接收到应答,且移动无线终端变为离开,则SGSN会存储用于该终端的旧和新P-TMSI。建议了两种解决方案来解决该问题:

解决方案1

移动无线终端14发起离开

为了使自身离开图1的无线电话网络,移动无线终端14向其对应的SGSN发送离开请求消息(Detach Type, P-TMSI, P-TMSI签名,断开)。根据该建议方案,移动无线终端14在离开请求消息中包括其旧P-TMSI。按照这种方式,SGSN得知哪一个P-TMSI存储在HLR 30中。

无线电话网络10发起离开

为了发起离开,SGSN向移动无线终端14发送离开请求消息。作为响应,移动无线终端14向SGSN发送离开接受消息。然而,利用网络发起的离开,当接收到请求或接受消息以去除P-TMSI含糊时,没有出现P-TMSI交换。UMTS 3GPP标准没有讨论P-TMSI重新分配

和网络发起离开冲突的可能性。典型地，无线网络 10 能够进行等待，直到从移动无线终端 14 向 SGSN 发送了 P-TMSI 重新分配完成应答消息。然后，当终端再次开启电源时，移动无线终端 14 向无线网络 10 发送离开请求消息，以避免含糊。在这种实例中，SGSN 在 HLR 中存储新的 P-TMSI。

解决方案 2

另一个建议的解决方案同时需要 SGSN 向 HLR 30 发送旧和新 P-TMSI。因此，在添附时，当被新 SGSN 请求时，HLR 30 能够将移动无线终端 14 曾经发送的 P-TMSI 映射到所存储的 IMSI。

前面说明了用于在添附到无线网络期间保护移动无线终端的身份的技术。

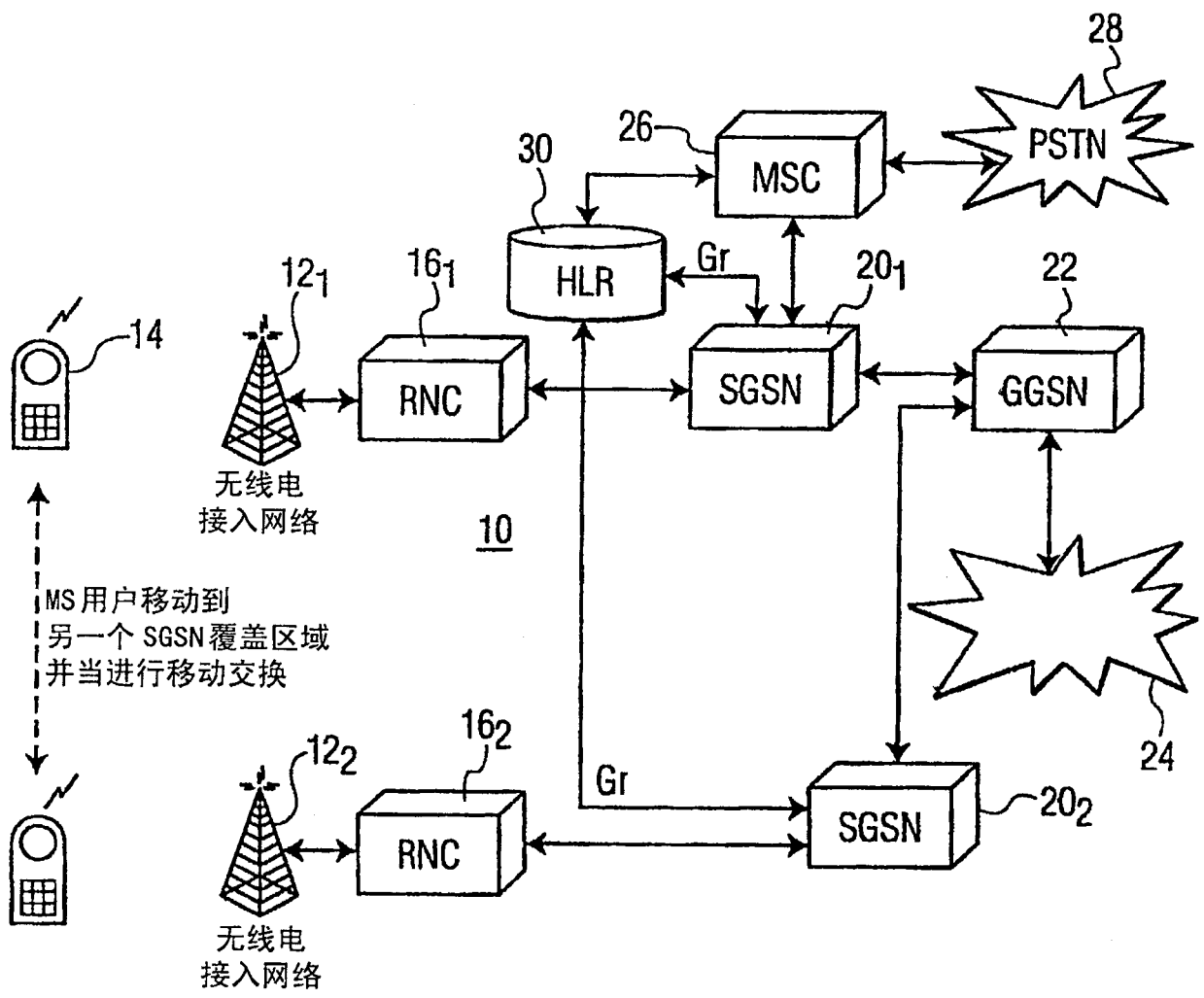


图 1

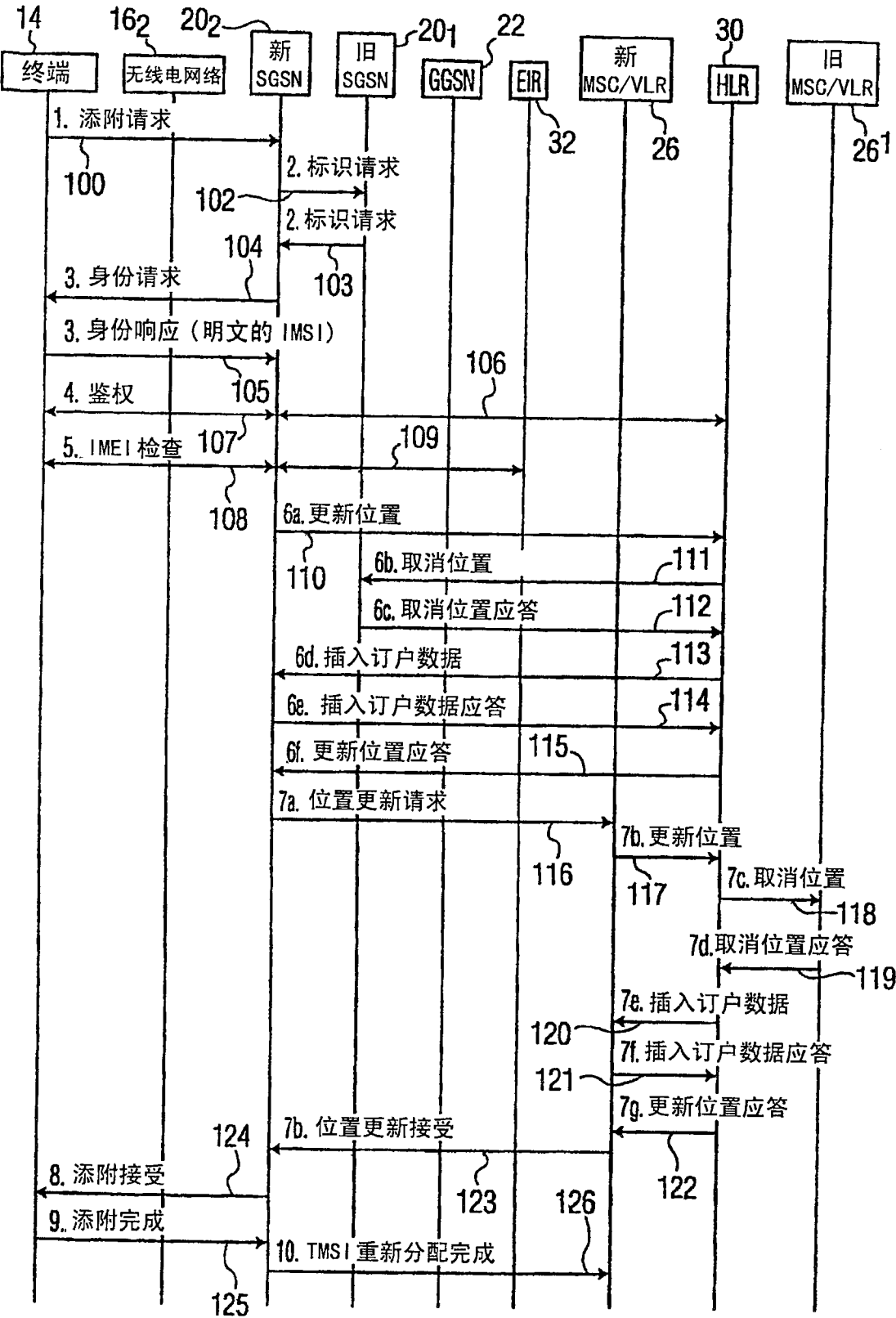


图 2

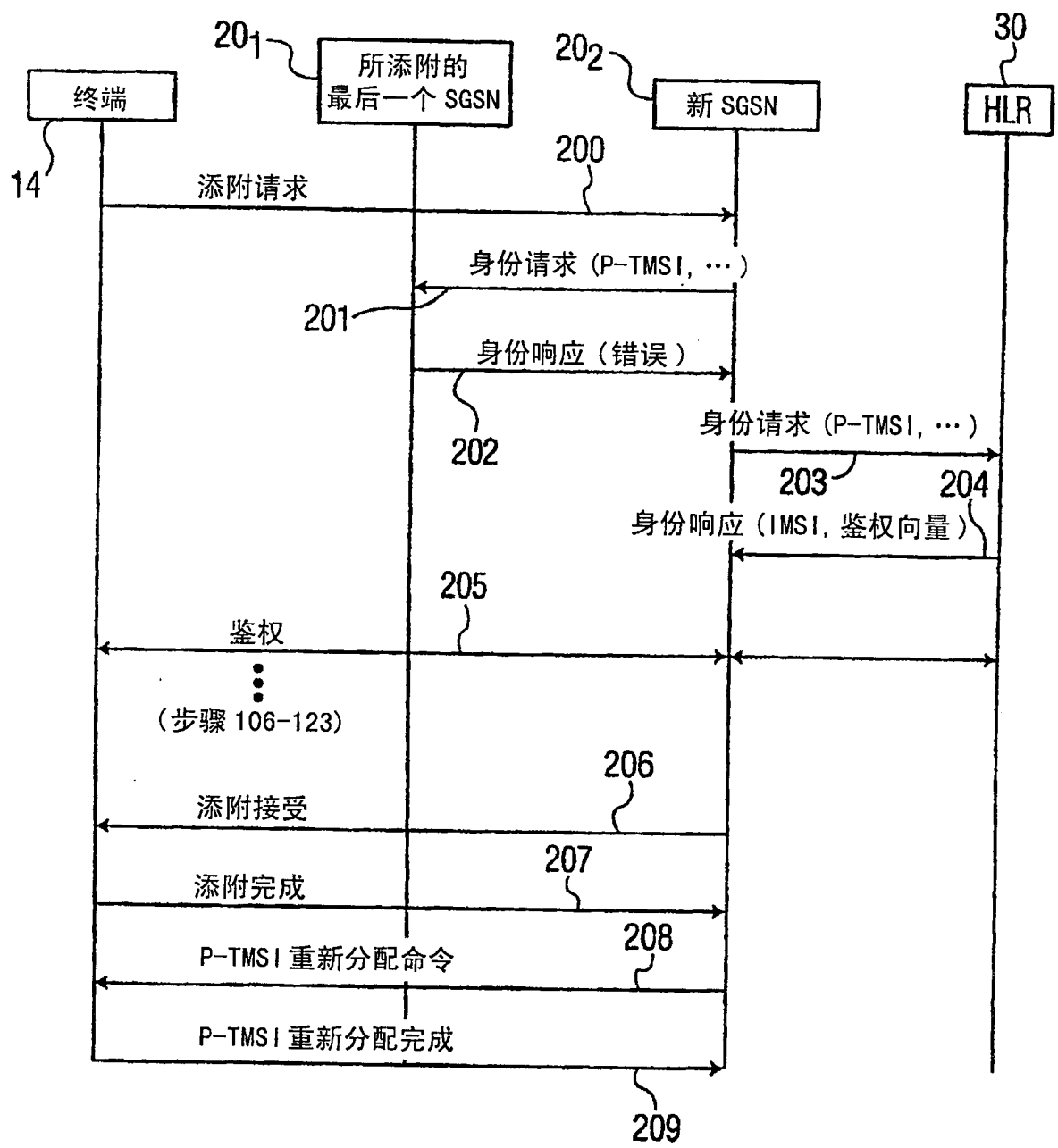


图 3